BROOKHAVEN NATIONAL LABORATORY

SBMS Interim Procedure

Interim Procedure Number: 2003-003 **Revision:** 1

Title: Official Use Only (OUO) Information Implementation at BNL

Point of Contact: Leonard Butera
Management System: Safeguards and Security Management System

Effective Date: September 5, 2003 **Expiration Date:** March 30, 2005

Approved by (line management, Management System Steward**):** Leonard Butera, Michael J. Bebon
Approved by (Deputy Director, Operations**):** Thomas R. Sheridan

Applicability: All BNL management, staff, guests, and visitors

Procedure:

1. Official Use Only (OUO) Information – What it is.

Unclassified information that has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activity may be considered Official Use Only if it meets the criteria for an exemption to the Freedom of Information Act (FOIA).

The Freedom of Information Act provides that any person has a right to obtain access to federal agency records, except to the extent that such records are protected from disclosure by one of nine exemptions. These nine exemptions are detailed in DOE G 473.3-1 available on the web at http://directives.doe.gov. A brief summary of the exemptions follows:

> Exemption 1: This covers National Security Information classified pursuant to Executive Orders. Since the information is classified Confidential, Secret, or Top Secret, it is never OUO.
>
> Exemption 2: Circumvention of Statute. This is information related solely to the internal personnel rules and practices of an agency. It can be of a relatively trivial nature or "low 2" such as a parking plan that is not deserving of OUO protection, or it could risk circumvention of a legal requirement which is known as "high 2." Some examples of "high 2" information that may warrant protection are vulnerability assessments, guidelines for conducting investigations, inspection and appraisal processes, materials used in determining personnel promotions, demotions, or transfers, and computer access codes.

Exemption 3: Statutory Exemption. This is information that Congress has decreed by law that is not releasable to the public. In DOE, the applicable law is the Atomic Energy Act which governs the formal control of classified Restricted Data and Formerly Restricted Data. It also governs the control of Unclassified Controlled Nuclear Information (UCNI). Since these areas are controlled and protected by statute, they are not Official Use Only. There are other areas, however, where statutes exist but no formal control systems are in place. They may be considered for control as OUO. Some examples are the Federal Technology Transfer Act, which covers Cooperative Research and Development Agreements (CRADAs), Export Controlled Information (ECI), Commodity Exchange Act, Patent Act, and numerous others.

Exemption 4: Commercial/Proprietary. This concerns trade secrets and commercial or financial information obtained from a person and that is privileged or business confidential. Some examples are bid, contract proposals, and related information received in confidence. Included are trade secrets, inventions, discoveries, etc. Contract performance, profit and loss, and expenditures from sub contractors or potential subcontractors are other examples.

Exemption 5: Privileged Information. This concerns inter-agency or intra-agency correspondence, which would not be available by law to a party other than an agency in litigation with the agency. The three primary privileges are deliberative process, attorney-client, and attorney-work product. The most important one within DOE is the deliberative process privilege. It protects predecisional information and deliberative information such as recommendations that have not yet been implemented. At first glance, exemptions 4 and 5 appear similar. The distinction is that exemption 4 pertains to information generated by a company and provided to the Government, while exemption 5 applies to Government generated information.

Exemption 6: Personal Privacy. This concerns personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Exemption 7: Law Enforcement. Some examples are manuals on law enforcement procedures, witness statements, identity of firms or individuals being investigated, other criminal investigation information, identification of confidential sources, information that may assist a criminal element, etc.

Exemption 8: Financial Institutions. Protects evaluations of a financial institution's stability, which may undermine public confidence.

Exemption 9: Wells. Rarely used but protects geological and geophysical information and data, including maps, concerning wells.

2. Who can identify OUO Information?

You can, as a DOE contractor. Your first responsibility is to ensure the information is not classified. If you are not sure, you must have the information reviewed by an authorized classifier. For a list of authorized classifiers at BNL look at www.bnl.gov/ssd/classifiers.asp.

3. Who can have access to OUO?

Anyone who has a need to know the information to perform their jobs or other DOE-authorized activities may be granted access to OUO information. The determination of need to know is made by the person possessing the OUO information, not the person requesting access. OUO is not releasable to the general public such as through the media.

4. How to mark OUO.

Front marking. The FOIA exemption number and category name must be placed on the front of an OUO document. Also, the name and organization of the person designating the information as OUO is placed on the front along with the date. If classification guidance is used to determine OUO, that information is also entered. A stamp, shown below, is normally used to apply this information.

OFFICIAL USE ONLY
May be exempt from public release under the Freedom of Information Act
(5 U.S.C. 552), exemption number and category_____
Department of Energy review required before public release
Name/Org:_____ Date:_____
Guidance (if applicable):_____

Page marking. The words "Official Use Only," or "OUO" if space is limited, are placed on the bottom center of each page that contains OUO information. Portion marking (marking each paragraph) is not required unless the document is classified National Security Information and also contains OUO portions.

Marking E-mail messages. The first line of an e-mail message containing OUO must contain the abbreviation OUO preceding the text. If only a message attachment is OUO, this must be indicated in the text and the attachment must be properly marked.

Restricted access files. These are medical and personnel records and similar files. They need not be marked OUO as long as they are maintained in files that have restricted access. They can be removed for reference, inventory, or similar purposes and returned to the restricted files without being marked. However, if a document is removed from these files and is not to be returned, it must be reviewed for OUO and marked if appropriate.

Transmittal document. A document that transmits an OUO document but does not itself contain OUO must be marked on the front as shown below to call attention to the presence of OUO information in the attachment or enclosure.

Document transmitted contains OUO information

Existing documents. You do not need to review your files for documents that may contain OUO information and mark them if they were generated prior to the implementation of the OUO directive (4-9-03). If they are to be considered for public release, however, they must be reviewed for the presence of OUO information and marked if appropriate.

5. Protecting OUO documents.

OUO information in any format must be kept under the control of the person possessing it or kept secure in a locked receptacle such as a room, filing cabinet, or desk. They should be destroyed by shredding in ¼ inch strips when no longer required. The Laboratory shredder in building 494 meets this criterion.

6. Transmitting OUO information.

By mail – outside of BNL. A sealed opaque envelope or wrapping should be used and the words "To be opened by addressee only" placed on the package. U.S. Mail or commercial carriers may be used.

By mail – within BNL. Same as above. Interoffice envelopes (holy Joes) are not sufficient without the opaque wrapper.

By telecommunications circuits. Protect by encryption whenever possible. Either a Secure Telephone Unit (STU) facsimile or the use of Entrust encryption is acceptable. However, if encryption is not available and transmittal by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document using the following procedures:

> An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when received. For e-mail, you may include the OUO information in a word processing file that is password protected and attached to the e-mail. The sender can then call the recipient with the password to access the file.

By voice. Use encryption (STU) if feasible. If not, then a regular telephone may be used.

Automated Information Systems (AIS). AIS must provide methods (e.g. authentication, file access controls, passwords) to prevent unauthorized access to OUO information stored on the system.

7. Other agency markings.

Provide the same level of protection and control over documents received from other agencies that contain OUO information. The Department of Defense (DoD) uses “For Official Use Only” (FOUO), the Department of State (DOS) uses “Sensitive But Unclassified” (SBU), and the Department of Justice (DOJ) uses “Limited Official Use” (LOU).